OGC REVIEW COMPLETED

22 August 1955

MEMORANDUM FOR: Office of Security

SUBJECT : Application of Crypto Security Law

1. This Office recently undertook a study of the Crypto Security Law (P.L. 513, 81st Cong., 18 U.S.C. § 798), with particular reference to its application to this Agency and the administrative practices and procedures of the Agency. This memorandum presents a brief analysis of certain portions of the law, together with several recommendations concerning practices of CIA and, to some extent, other agencies and departments. It should be realized, however, that the legal points are not beyond argument. What is intended here is to suggest certain steps which the Agency might be well advised to take in order to strengthen the Government's case in the event a prosecution under the Act is brought.

2. The purpose of Section 798, which is included in the Espionage chapter of Title 18, is stated in the title of P.L. 513 as follows:

> "To enhance further the security of the United States by preventing disclosures of information concerning the cryptographic systems and the communication intelligence activities of the United States."

The substance of the Act, set out in sub-section (a) of Section 798, is that one commits an offense who knowingly and willingly:

> "communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information -
>
> (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government [hereinafter referred to as CRYPTO];
>
> (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes [hereinafter referred to as CRYPTO devices and COMINT devices, respectively];

(3) concerning the communication intelligence activities of the United States or any foreign government [hereinafter referred to as COMINT];

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes [hereinafter referred to as COMINT] . . ."

Then follow several definitions, including:

"The term 'classified information' means information which, at the time of a violation of this section is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms 'code', 'cipher', and 'cryptographic system' include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term 'communication intelligence' means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term 'unauthorized person' means any person who, or agency which, is not authorized to receive information of the categories set forth in sub-section (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States."

3. Classified Information.

(a) Section 798 affords greater protection, in its field, to the United States, with respect to the passing of information to unauthorized persons, than do the other espionage laws (Sections 793 and 794 of Title 18) in that the intent of the accused is not significant. Under Sections 793 and 794 an intention to injure the United States, or reason to believe that the information is to be used to injure the United States or to the advantage of a foreign power, is required. Under Section 798 the accused need only have willfully and knowingly passed classified information to an unauthorized person.

(b) Section 798 also differs from Sections 793 and 794 in the definition of the information the passage of which involves an offense;

the latter two concern "information respecting the national defense" and "information relating to the national defense", as contrasted with information which "is, for reasons of national security, specifically designated by a United States Government agency for limited or restricted dissemination or distribution". The former language was held by the Supreme Court of the United States, in Gorin v. U.S. 312 U.S. 19, 61 S. Ct. 429, to involve a question of fact, that is, the jury must determine whether the acts of the defendant "are connected with or related to the national defense" (61 S. Ct. 436). Thus, in prosecutions under those sections it is necessary to prove connection with the national defense, a requirement which could be embarrassing, if applied to information classified "for reasons of national security", since in such cases the prosecution would have to submit the very information (and presumably much more) the dissemination of which had been restricted by an agency of the Government "for reasons of national security".

Although it is not free from doubt, it is believed that under Section 798 it would not be necessary to submit to the jury, or to prove, the question of whether the designation "for reasons of national security" was a correct one; proof that the designation was made and that the agency which made it did so for reasons which the agency regarded as "reasons of national security" should be all that is required. The information which is pertinent under Sections 793 and 794 is referred to in those sections by a generic term - information "respecting the national defense" or "relating to the national defense". Information which is the basis of an indictment may or may not fall within the generic term; someone's opinion (the jury's) must be obtained and accepted. The phrase by which Section 798 refers to the information which is significant thereunder covers information with respect to which a particular action has been taken, i.e., information which a government agency has specifically designated a certain way for a certain reason. The only question requiring an opinion by the jury is whether such action occurred, not whether it should have occurred. Any contention to the contrary is believed refuted by the fact that its acceptance would render the statute unenforceable in many cases, since security considerations doubtless would preclude the Government from introducing into evidence information to establish "reasons of national security". Since the plain intent of the statute is to protect the COMINT and CRYPTO systems by establishing offenses and punishments for the violation thereof, an interpretation which would defeat such intent should be avoided.

In any event, if the above analysis is incorrect, that is, if the jury would be allowed to judge whether the Agency correctly designated information "for reasons of national security" there appears to be nothing to be done about it except to decide, whenever a case is ready to go to trial, whether we are prepared to make available records and information to be introduced as evidence. But in order to take advantage of the statute in the event the above analysis is correct, it is believed we would be well advised to designate documents in the language of the statute. For this purpose, a stamp reading as follows, could be used:

> "For reasons of national security, this document is specifically designated by the Central Intelligence Agency for limited or restricted dissemination or distribution."

Alternatively, the same result perhaps could be achieved by a regulation which all COMINT (or CRYPTO) cleared people would read; they would also certify to the same. The regulation, in addition to making reference to Section 798, would provide that all COMINT (or CRYPTO) documents will bear a named code word, or one of a series of code words that the dissemination or distribution of any document bearing any of the code words is limited and restricted by the Central Intelligence Agency for reasons of national security.

4. DD/P Pouching System.

The definitions of the terms "code", "cipher" and "cryptographic systems" (see paragraph 2 above) include "any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance or meanings of communications". This would appear broad enough to include not only our

25X1 [redacted]

might be well to utilize a regulation along the lines of that mentioned in paragraph 3(b) above.

5. Unauthorized Person.

A problem also arises with respect to the definition of "unauthorized person", namely a person or agency not authorized by the President or by the head of an agency designated by the President to engage in communication intelligence activities to receive CRYPTO or COMINT information. By directive, a number of agencies have been designated as the only agencies authorized to engage in COMINT activities. Other agencies of the Government, however (for example, those represented on the USCSB), utilize telecommunications. To the extent, if any, that the activities of any of these agencies require the receipt of information involving CRYPTO or COMINT or CRYPTO or COMINT devices it would appear necessary for the President, or the head of one of the agencies which is authorized to engage in COMINT activities, to authorize that agency and its employees to receive such information.

25X1A9A [redacted]

Assistant General Counsel

OGC:RHL:ms

Distribution
Orig. & 1 - addressee
Subject
Signer
Chrono
cc: DD/P
cc: Office of Communications
cc: Executive Sec., U.S. Communications Intelligence Board
cc: Executive Sec., U.S. Communications Security Board